

## SYSTEM AND METHOD FOR NETWORK SECURITY

### RELATED APPLICATION

The present application claims the benefit of U.S. Provisional Application Serial No. 60/463,268 filed April 16, 2003.

5

### FIELD OF THE INVENTION

The present invention is directed to an Internet security system. More particularly, the invention is directed to a security system for monitoring electronic communications between a user interface and any physical network.

### BACKGROUND OF THE INVENTION

10

The unrestricted and public transmission of material and ideas is one of the hallmarks of the Internet. Unfortunately, these inherent strengths of the online world are also often regarded as one of the Internet's greatest weaknesses. For example, the ability to easily obtain adult material is often cited by parent groups as a very significant problem with the online world. As a result, various systems have been developed in an effort to monitor and control access to online materials.

15

However, while the monitoring of static online material such as pictures and the like is important, of still greater concern is the ability of people to directly communicate with each other. In online forums (e.g., Internet chat rooms, instant messages), where the participants are typically anonymous or have created fake identities, all participants are permitted to discuss events in writing and in real time.

20

This direct link between participants creates the obvious and real danger that individuals participating in these online communications may attempt to contact children and then lure them into harm's way.

5        Additionally, it is known that modern day terrorists use the Internet to communicate and to plan attacks in attempts to subvert national security. It is appreciated that many of these types of communications go virtually unnoticed only to be revealed after a planned attack has been executed.

10        On the corporate front, faster, cheaper, and wholly networked portable computers have provided companies with the tools to network employees and to provide global resource access, thus making for a virtual workplace. While, on the one hand, this can provide a critical competitive position, it also provides unprecedented exposure to corporate espionage and intellectual property theft.

15        Therefore, there is a need for a system that monitors electronic communications (e.g., e-mail, Internet chat rooms and instant messages) and permits an administrator to notify authorities of any suspicious behavior on the part of any participant to the communication.

## SUMMARY OF THE INVENTION

20        The present invention provides a system and method for use in combination with an Internet service provider, or as a standalone system used in corporate environments, for monitoring electronic communications conducted via the Internet or Intranet. The Internet service provider or corporate entity is provided in

communication with a server for storing communications that are determined to be inappropriate based on predetermined criteria. The system allows for Internet/Intranet communications to be automatically and continuously monitored, and allows for predetermined entities to be automatically alerted when the monitored  
5 communications are determined to be inappropriate based on predetermined criteria.

The system includes a user interface in communication with the Internet service provider or corporation whereby communications between a user and at least one other party is facilitated via the Internet/Intranet.

A software program employed by the Internet service provider or corporation  
10 is operative to monitor the electronic communications between the user interface and the Internet/Intranet and to cause the electronic communications corresponding to inappropriate communications to be sent to the server when the monitored communications satisfy a predetermined criteria. The server stores the portion of the electronic communications and thereafter automatically generates a violation notice  
15 regarding the monitored communications considered to be inappropriate.

A content administrator is in communication with the server for receiving the violation notice and for accessing the stored electronic communications that are determined to be inappropriate based on the predetermined criteria. The system permits the content administrator to send complaint information to the authorities  
20 when the content administrator determines that the stored electronic communications are in fact considered inappropriate communications upon review.

The present invention provides the advantage of providing a user with a means for being alerted automatically to inappropriate communications being conducted between a user interface and the Internet/Intranet. In this manner communications related to criminal conduct or planning can be realized before harm  
5 occurs. Additionally, the user is allowed to selectively alert legal authorities of the potential criminal conduct for further investigation without the parties being aware that the authorities have been notified.

#### BRIEF DESCRIPTION OF THE DRAWINGS

A better understanding of the present invention will be had upon reference to  
10 the following detailed description when read in conjunction with the accompanying drawings in which like parts are given like reference numerals and wherein:

Figure 1 is a diagrammatic view of the Internet security system as according to the invention;

Figure 2 is a process flow diagram of a preferred embodiment of the Internet  
15 security system as according to the invention;

Figure 3 illustrates a diagrammatic view of an alternative embodiment of the Internet security system as according to the invention; and

Figure 4 illustrates a process flow diagram of the alternative embodiment of the Internet security system as according to the invention.

## DETAILED DESCRIPTION OF THE INVENTION

Referring to Figure 1, there is shown a preferred embodiment of an Internet security system 10 as according to the invention. Preferably the Internet security system 10 includes a user interface that is in communication with an Internet service provider (ISP) 14 that operates to facilitate communication between the user interface 12 and the Internet domain 20. Accordingly, communications data flow 22 between the user interface 12 and the Internet 20 passes through the Internet service provider's 14 facilities.

Preferably the user interface 12 is a personal computer. However, it is appreciated that other interfaces may be used such as handheld organizers, palm computers, pocket computers, cell phones or the like that are capable of facilitating communications via open networks such as the Internet.

Referring again to Figure 1, the Internet service provider includes at least one server 18 operative to store communications data 22 that pass through the Internet service provider 14.

A software program employed by the Internet service provider is disposed on a server 18 in communication with the Internet service provider 14. The software and server cooperate to monitor electronic communications between the user interface 12 and the Internet 20. The software program causes the communications data 22 to be stored on the server 18 when the monitored electronic communications are determined to satisfy predetermined criteria. The predetermined criteria may be

provided as a word or a group of words predisposed within the software program or words selectively provided by a user of the system 10. It is appreciated that the system may be adapted to monitor criteria other than words such as images, symbols and the like.

5           Upon determining that the monitored communication's data 22 is inappropriate, the server 18 stores the information and then generates a violation notice 24 for sending to a content administrator 26. Preferably, the violation notice 24 includes an electronic link that allows the content administrator 26 to remotely access the stored electronic communications at the server 18 that were determined to  
10   be inappropriate communications based upon the predetermined criteria. After the content administrator 26 has reviewed the stored electronic communications at the server 18, the system 10 allows the content administrator 26 to send complaint information 28 to legal authorities 30 such that further investigation may be conducted or other appropriate action may be taken.

15           As mentioned briefly above, the system 10 preferably allows for a content administrator 26 to customize the predetermined criteria used by the software program for monitoring communications data 22. Furthermore, preferably the software package allows for the content administrator 26 to selectively set the system  
10   up for a particular level of communications monitoring such as low, medium or  
20   high levels of monitoring. It is appreciated that the higher security levels result in a greater level of scrutiny during the monitoring of communications data 22.

As an alternative to the violation notice including an electronic link that permits a content administrator 26 to access the stored portion of the electronic communications 22 at the server 18, the violation notice may include vital information concerning particulars of the communication illustratively including the user names of parties involved in the communication, a portion of the communications, e-mail addresses, the time and date of the communications. Most preferably, each violation notice 24 includes an electronic link that allows the content administrator 26 to cause the server 18 to automatically generate and send a complaint 28 to legal authorities 30 if the content administrator determines the stored communications to be of an inappropriate nature after review.

Referring now to Figure 2, a process flow of the preferred embodiment of the Internet security system is generally illustrated at blocks 50-70.

At block 50, the system software employed by the ISP operates to monitor the communications data 22 being transmitted between the user interface and the Internet 20. The process advances from block 50 to block 52.

At block 52, the software determines whether the communications data 22 satisfies the predetermined criteria that is predisposed in the software or selectively provided by the content administrator 26. The software continues to monitor communications until the predetermined criteria is satisfied. The method of the Internet security system as according to the invention then advances from block 52 to block 54.

At block 54, the software operates to cause the server to store a portion of the entire electronic communications data 22 that satisfied the predetermined criteria, and at block 56 the system operates to generate a violation notice that is sent to the content administrator 26. The process continues from block 56 to block 58.

5           At block 58 the content administrator 26 receives the violation notice 24 and accesses and reviews the stored communications at the server 18 to determine whether the communications are in fact considered to be inappropriate communications. If the communications are determined to be harmless by the content administrator 26, then no action is taken and the system continues to monitor  
10       communications data 22 as according to blocks 50 and 52. If the content administrator 26 determines the communications data 22 provided in the violation notice 24 to be inappropriate, then the violation notice allows for the content administrator to cause the system to generate a complaint or alert message to be sent to legal authorities 30 by simply clicking the electronic link in the violation notice 24  
15       (see block 60). Thereafter, the legal authorities may continue the investigation or implement other appropriate action. It is appreciated that the option to alert authorities may be provided to the content administrator upon accessing the stored communications data at the server rather than in the violation notice.

          The system 10 as according to the present invention allows a content  
20       administrator 26 to access the server 18 from remote locations such that the content administrator may set up, reconfigure, modify or disable the features of the software



program relative to communications data monitoring criteria and/or the security level at which the communications data 22 is to be monitored.

Referring now to Figure 3, an alternative embodiment 10' of the Internet security system as according to the invention is provided.

5           The system components include a user interface 100 in communication with the Internet 110, a security server 120, and a content administrator 130.

          In this embodiment the software program 102 is disposed on a user interface wherein the software operates to monitor the communications data 22 between the user interface 100 and the Internet in a manner virtually unnoticed by the user of the  
10       interface 100. The user at the user interface 100 is permitted to receive data 104 and view data 106 as he or she normally would when communicating with an anonymous party at the Internet 110.

          The software 102 disposed on the user interface 100 monitors the data until the communications data is considered to be of an inappropriate nature relative to a  
15       predetermined criteria as according to the invention. When the communications are determined to be inappropriate, the software operates to send a portion of the monitored data 108 to the security server 120 where the information is received 122 and stored at 124.

          At the security server 120 the system 10' operates to generate a violation  
20       notice for sending to the content administrator 130. The content administrator 130 receives the violation notice 132 and thereafter accesses the stored data 124 at the

security server 120. The security server 120 displays the content 136 of the communications stored in the security server regarding the inappropriate communications. If the content administrator 130 determines the stored data to be inappropriate, then the system 10' allows for the content administrator 130 to cause the security server 120 to generate complaint information for sending to legal authorities at 140. The security server 120 may be adapted to be accessible by law enforcement authorities for permitting the authorities to review the stored data 124 relative to inappropriate communications. Optionally, the system allows for the real-time assumption of an identity by law enforcement personnel for the purpose of investigation and response. This is useful when law enforcement has been notified of an offender and said offender has been tagged by our system as a real and dangerous threat. Law enforcement personnel can assume an identity and correspond with the offender thereby gaining evidence.

Figure 4 illustrates a process for the alternative embodiment 10' of the Internet security system as according to the invention. At 150 the system software disposed on the user interface monitors electronic communication between the user interface and the Internet.

At 152 the system software recognizes the electronic communications to be of an inappropriate nature based upon the predetermined criteria. At 154 a portion of the communications data that is considered to be of an inappropriate nature as according to the predetermined criteria is sent to the security server for storage. In

this manner the operator at the user interface 100 cannot destroy the information as would be possible if the information were stored at the user interface 100.

At 156 the system server generates a violation notice and sends the notice to a content administrator. At 158 the content administrator is allowed to access the  
5 stored information at the security server for review. If the stored communications are considered to be inappropriate, the content administrator is allowed to cause the system server to generate a complaint message for sending to the local authorities. As described above, the content administrator preferably causes the complaint message to be generated by simply clicking an electronic link provided by the system  
10 10'. The Internet security system of the present invention provides advantages over conventional methods of cyber surveillance such as screen scraping wherein all communications data between a user interface and the Internet are stored on a portion of the monitoring system. This method creates huge log files of communications data which may or may not contain inappropriate communications and which could  
15 potentially take hours to review when attempting to discover such inappropriate communications.

In a corporate environment the system can be implemented by installing the software on a server disposed at the corporate facility for continuously monitor all network communications over the Intranet/Internet. The security server is  
20 disposed off-site at a remote facility controlled by a network security service provider

that supports the system. It is appreciated that system provides for communication with a content administrator and legal authorities as according to the foregoing.

Alternatively, the system may be implemented as a standalone system whereby the entire system resides within the corporate boundary. That is to say that a  
5 server that runs software and the security server including storage facilities operate at the corporate site.

Preferably, the present invention only stores communications that are determined to be inappropriate based on the predetermined criteria that is provided as part of the software and/or selectively provided by the content administrator. Further,  
10 the system prevents one who is alerted to his or her communication being monitored from destroying content of the electronic communications because the information is always stored remotely from the user interface at all times. Still further, the present invention allows for the content administrator to selectively review portions of the electronic communications to determine if the communications are in fact considered  
15 to be of an inappropriate nature and to thereafter automatically cause a complaint message to be sent from the system to legal authorities as necessary. The system allows for the real-time assumption of an identity by law enforcement personnel for the purpose of investigation and response.

From the foregoing, the present invention provides an Internet security system  
20 for monitoring communications between a user interface and an anonymous party communicating over the Internet/Intranet. One skilled in the art upon reading the

ITL-10002/08  
40412gs

specification may come to appreciate changes and modifications that do not depart from the spirit of the invention as defined by the scope of the appended claims.

I claim: